

particular to the good, which would allow one to verify the authenticity of the good. The Examiner noted that the claimed invention was "not incredible". However, the Examiner is reminded that incredibility is not the test for *prima facie* obviousness. Indeed in order to be patentable all that needs to be claimed is that which is useful and not taught or suggested in the prior art. The Examiner further suggested that a reason it may not be shown in the prior art is that in the past smart cards were too expensive, but now that smart cards are cheap the invention is obvious. However, it is improper to speculate as to why something may or may not have been discovered sooner. Moreover, the reason that it is not shown in the prior art is immaterial to patentability. If it is not taught or suggested by the prior art, no matter the reason, Applicant is entitled to a patent.

Further during the course of the conversation, the Examiner indicated that his art unit deals with e-commerce cases which, with all the recent publicity, are subject to additional levels of review once allowed by the Examiner. The undersigned noted that this case was not e-commerce *per se*, but rather a system for verifying the authenticity of manufactured goods using smart cards. However, regardless of whether or not the Examiner considers this case an e-commerce application, the standard of review remains the same. The Examiner is reminded that while e-commerce cases may be subject to multiple levels of review, they are not subject to a lower showing of *prima facie* obviousness under § 103.

Below are Applicant's remarks responsive to the Office Action. The remarks were used as a point of discussion during the interview.

REMARKS

Claims 1-21 remain presented for reconsideration. Applicants note with appreciation the Examiner's indication that the previous grounds of rejection have been withdrawn.

It is respectfully noted that the rejections in the present Office Action

are awkwardly organized and it is therefore difficult to determine the exact grounds of rejection to fashion a response. However, as best as can be determined, the lengthy new grounds of rejection have been presented in the present Office Action as follows:

1. Claims 1, 5-6, 8-10, and 15 stand rejected under 35 U.S.C. § 103 as being unpatentable over the article "Fuji-Keizai USA, Inc." (hereinafter "Fuji"). The Examiner also refers Applicants to USP 5,901,303 to Chew, although not specific rejection has been articulated using Chew;
2. Claim 2 appears to be rejected under § 103 as being unpatentable over Fuji further in view of Chew, although again, the Examiner has provided no analysis or reasoning with regard to Chew;
3. Claim 3 appears to be rejected under § 103 Fuji in view of USP 5,367,148 to Storch, although not explicitly stated as such;
4. Claim 4 stand rejected under 35 U.S.C. § 103 as being unpatentable over Fuji in view of USP 5,740,250 to Mob;
5. Claims 7 and 17 stand rejected under 35 U.S.C. § 103 as being unpatentable over Fuji in view of USP 5,140,634 to Guillou;
6. Claim 11 stands rejected under 35 U.S.C. § 103 as being unpatentable over Fuji in view of USP 5,367,148 to Storch;
7. Claim 12 appears to be rejected under 35 U.S.C. § 103 to Fuji alone;
8. Claims 13 and 20 appear to be rejected under § 103 as being unpatentable over Fuji in view of USP 5,971,435 to DiCesare;

9. Claims 14 and 19 stand rejected under 35 U.S.C. § 103 as being unpatentable over Fuji in view of USP 5,164,988 to Matyas; and

10. Claims 16 and 21 are indicated as being rejected for the same reasons as claims 1-15 above. However, claims 1-15 have been rejected on many separate grounds. Hence, this rejection is not readily understood. However, it is assumed in good faith that claims 16-21 are rejected over Fuji alone.

These rejections are respectfully traversed based on the following discussion.

Briefly, the present invention is directed to verifying the authenticity of manufactured goods using a smart tag attached to the goods containing encrypted authentication information. The authentication information may comprise, for example, a serial number, a description of the good's physical appearance or chemical composition, its color, digital images of the good, etc. The encryption procedure comprises public/private key encryption with zero-knowledge protocols. Zero knowledge protocols allow a smart tag to be authenticatable and yet be duplication resistant by allowing the verifying agent to convince him/herself that the smart tag is authentic without revealing its authentication information. The verification procedure can be done using a reader at a point of sale (POS) machine equipped with the appropriate public key and zero-knowledge protocols to decrypt the authentication information. A printed version of the serial number or other authentication information may be placed on the goods in human readable form to quickly verify the information electronically read from the smart tag. With the present invention, only the manufacturer can create such smart tags with the associated data thus making it virtually impossible to pass off a counterfeit good as authentic. In addition to authenticating counterfeit goods, the present invention can be used to detect authentic goods being sold in a parallel market.

Despite the large number of references used by the Examiner to reject the claims, all rejections are based on the primary reference to Fuji. It is

respectfully submitted that Fuji is absolutely unrelated to using smart cards to authenticate goods or to identify counterfeit goods. Further, none of the secondary prior art, relied on by the Examiner in combination with Fuji, remotely teaches or suggests using a smart card to authenticate goods to detect counterfeits.

The title of the Fuji is "Top 40 High Tech Companies in Europe: Gemplus, France, Analysis of Factors/Strategies for Company's Success, Future Plans and Business Opportunities in the Industry". As the title implies, the article is about the Gemplus Company who is apparently a company in the business of manufacturing smart cards and smart card readers. The article indicates that smart cards are used in a number of various applications including computer security, information highways, healthcare, banking, telecommunication, and instant encryption and decryption of data. However, the article does not teach or suggest attaching a smart card to a product or good such the authenticity of the good can be readily verified.

Similarly, Chew is directed to smart cards and more particularly to reducing card /reader interface complexity. With the reduced complexity, Chew suggests that smart cards may be designed into mobile phones, prepaid telephone cards, electronic purses, pay TV, etc. (see, column 3, lines 45-61). Again, nothing in Chew, alone or in combination with Fuji, teaches or suggests attaching a smart card to a product or good such the authenticity of the good can be readily verified.

Matyas is directed to a public/private key encryption system. As discussed in column 8, lines 50 *et seq.*, "A network is configured so that a first data processor provides a certification center function for the network. A second data processor in the network functions as client device A, which will seek certification of its public keys by the certification center. A third data processor in the network functions as client device B, which will seek certification of its public keys by the certification center. In accordance with the invention, the certification center will encode the network security policy into a configuration vector which is transmitted to each client device A and B

in the network".

Matyas thus has absolutely nothing to do with smart cards and does not, alone or in combination with Fuji, teach or suggest attaching a smart card to a product or good such the authenticity of the good can be readily verified.

DiCesare is directed to a method for verifying the authenticity of an autograph. DiCesare requires that when a celebrity autographs an item, a person witnessing the autograph provides a numbered certificate of authenticity, and thereafter stores the number in a database. Again, nothing in DiCesare, alone or in combination with Fuji, teaches or suggests attaching a smart card to a product or good such the authenticity of the good can be readily verified.

Guillou is directed to a signing messages using zero-proof protocol and verifying the authenticity of banking or smart cards using zero-knowledge proof protocols. However, nothing in Guillou, alone or in combination with Fuji, teaches or suggests attaching a smart card to a product or good such the authenticity of the good can be readily verified.

Mob is directed to a tame automorphism based encryption system or scheme. Other than mentioning public and private key encryption, Mob is unrelated to the present invention. That is, nothing in Mob, alone or in combination with Fuji, teaches or suggests attaching a smart card to a product or good such the authenticity of the good can be readily verified.

Storch is directed to counterfeit detection using ID numbers having a random portion. The randomness of the ID numbers makes it difficult for a counterfeiter to anticipate the numbers. Unlike the other references cited by the Examiner, at least Storch is directed to identifying counterfeit products. However, nothing in Storch, alone or in combination with Fuji, teaches or suggests attaching a smart card to a product or good such the authenticity of the good can be readily verified.

Referring the Examiner now to MPEP § 2143, titled "**Basic Requirements for a *Prima Facie* case of Obviousness**", the MPEP mandates that:

"To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine the reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all of the claimed limitations.

The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not applicant's disclosure." (emphasis added).

Claim 1 recites "A system for verifying authenticity of a manufactured product, comprising: an electronic tag attached to one of said product and product packaging, said electronic tag comprising a memory for storing authentication information for said product in encrypted form; and a reader equipped with a decryption key for reading said authentication-information from said electronic tag to verify that said product is authentic" (emphasis added).

Similarly, independent claim 16 recites "A method for verifying the authenticity of a manufactured product, comprising the steps of: generating authentication information for a manufactured product; encrypting said authentication information using a private key; storing said encrypted information in electronic tag; attaching said electronic tag to one of said manufactured product and manufactured product packaging; reading said encrypted authentication information from said electronic tag; and decrypting said encrypted information using a public key corresponding to said private key to verify that said manufactured product is authentic" (emphasis added).

Here, Applicants are claiming smart cards (e.g., electronic tags) for a specific purpose. That is, they are attached to goods in order that a consumer or law enforcement agency can readily tell whether or not the good is

counterfeit (i.e., to verify authenticity). The Examiner has cited Fuji which teaches nothing more than the existence and popularity of smart cards. However, Applicant's are not claiming to be the first to invent smart cards. Indeed, as Fuji and Chew shows, smart cards have been around for some time. The Examiner has relied on Matyas, Guillou, and Mob for teaching that various encryption methods are know. However, again, Applicant is not claiming to be the first to invent encryption, indeed encryption has been around for years. The Examiner has relied on DiCesare and Storch for teaching various methods for verifying the authenticity of a good. However, none of these methods teach or suggest using electronic tags to verify the authenticity of a good.

With regard to claim 21, the Examiner has provided absolutely no bases for rejecting this claim directed not to verifying the authenticity of a good, but rather identifying an authentic good being sold in a parallel market (i.e., a good wrongfully sold or resold in a high priced market).

Based on the above discussion, it is respectfully submitted that the prior art cited by the Examiner does not make out a case of *prima facie* obviousness as required under § 103 and it is respectfully requested that the prior art rejections to the claims be withdrawn.

In view of the foregoing, it is respectfully requested that the application be reconsidered, that claims 1-21 be allowed and that the application be passed to issue.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone number listed below to discuss any other changes deemed necessary in a telephonic interview.

Please charge any deficiencies in fees and credit any overpayment of fees to Attorney's Deposit Account No. 50-0510 (IBM/Yorktown).

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Kevin A. Reif". The signature is fluid and cursive, with the first name "Kevin" being more prominent than the last name "Reif".

Kevin A. Reif
Reg. No. 36,381

McGuireWoods LLP
1750 Tysons Boulevard
Suite 1800
McLean, Virginia 22102
(703) 712-5000